**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 294**

Security Equipment

**Security Software**

Describe each of the following software-based security types.

1. Encryption software
   1. What are the two types of modern encryption methods?

* Symmetric-key encryption
* Asymmetric-key encryption

1. Network policies, profiles

In some cases, staff members may be located in different parts of the world, but working on the one document (group collaboration)

1. Firewalls

Is a type of network protection, used to restrict access by outsiders to a network, as well as to protect confidential info.

1. Antivirus software

Used to prevent computer virus infections.

**Security Procedures, p 299**

**Communication:**

1. List the security considerations for communication within an organisation.

* Well-documented processes for communicating sensitive information via email, telephone and fax
* Use of passwords on documents that have sensitive information
* Well-documents policy for the use of networked devices within the organisation.

**Storage**

1. **Filenaming conventions**
   1. List the 3 types of information each document should include.

* File-naming convention
* Location of files
* Backup procedures, strategies and timelines
  1. Give an example of a sequential file-naming convention.

Should contain the date of the document, the version of the document and the name should be meaningful.

1. **Location of files**

When storing files on a network server, an organisation set a directory structure to control where employees store their files so documents can be easily located when needed.

1. **Backups**
   1. Distinguish between each of the following:
      1. Full backup

Copies all files and should be done weekly, fortnightly or monthly.

* + 1. Differential backup

Copies only files that have been changed since the last full backup

* + 1. Incremental backup

It is similar to the differential back up but two or more medias are used.

1. **Backup timeline**
   1. List good practice in relation to backup timelines.

It is good practice to label all backup media so that you know when the backup was made and what it was on. Al log may also be kept of the by a systems manager recording the dates of backup, the location of files and whether or not any restorations have been made.

1. **Location of backup files**
   1. List good practice in the relation to the storage of backup files.

Your backups should be stored in a location that is safe from theft, and damage caused by extremes of temperature or disasters.

* 1. What is the grandparent-parent-child system?

A suggested backup routine known as the grandparent-parent system. The parent is the second oldest copy of the file. The child is the most recent copy of the file. An incremental backup is performed each day, with a differential backup at the end of each week. A full back is done at the end of each month.

1. **Archiving and destruction**
   1. Distinguish between archiving and destruction?

Archiving is essentially a process of copying files to long-term storage, then deleting them from the hard disk. Destruction involves deletion only.

* 1. What is a problem for ICT managers?

The problem is determining which is the most appropriate long-term storage medium to use.

* 1. What is a legacy system?

These systems might run old databases on old servers or mainframes.

1. **Disposal**
   1. What issues must organisations consider in disposing information?

When disposing of information organisations must consider protection sensitive data (there are currently many ways of ‘deleting’ data from a storage medium as none of them can completely guarantee that information is completely disposed of).